REMARKS

Claims 2-4, 7-12, 14, 16, 18-21, 23, 25-33, and 36-38 remain pending in the present application as amended. Claims 30 and 31 are independent[1] and have been amended, as have dependent claims 37 and 38. No claims have been canceled or added. Applicants respectfully submit that no new matter has been added to the application by the Amendment. In particular, the code ID as now recited in claims 30 and 31 is disclosed paragraphs [0025]-[0028] and Fig. 2 of the application as filed, and the first computer entity being an executable is disclosed in paragraphs [0003] and [0038] of the application as filed.

Telephone Conversation With Examiner

Examiner Johnson is thanked for the telephone conversation conducted on March 18, 2010. Proposed amendments were discussed. Asserted art was discussed. It appears that the proposed amendments advance prosecution.

Section 112, 1st paragraph Claim Rejection

The Examiner has rejected claims 37 and 38 under 35 USC § 112, 1st paragraph for the reason that the claims are believed to include new matter. Applicants respectfully traverse the Section 112, 1st paragraph rejection insofar as it may be applied to the claims as amended. According to the Examiner, 'unencrypted' in claim 37 and 'preclude' in claim 38 are not believed to be supported by the specification as filed. Without prejudice or disclaimer, Applicants have removed such terms from such claims, and instead have recited that the messages of claims 37 and 38 are transmitted 'without encryption'.

Applicants respectfully submit that transmitting the messages 'without encryption' is indeed supported by paragraph [0054] of the application (as filed), which states that "inasmuch as the [information in each message] is likely not of a sensitive nature, such [information] need not necessarily be encrypted". In particular, Applicants respectfully point out that the relevant

[1] The Examiner states in the Office Action that claim 19 is independent also. However, claim 19 presently depends from claim 30.

public would surely appreciate that 'without encryption' can be reasonably inferred from 'need not necessarily be encrypted'. As a result, Applicants respectfully request reconsideration and withdrawal of the Section 112, 1st paragraph rejection.

Section 103 Claim Rejections

The Examiner has now rejected claims 2-4, 7-12, 14, 18-21, 23, 25-27, 29, 31-33, and 36-38 under 35 USC § 103 as being obvious over Yan et al. (U.S. Patent Pub. No. 2005/0033987) in view of Qui (U.S. Patent Pub. No. 2004/0148505) and further in view of Pinkas et al. (U.S. Patent No. 5,214,700), claims 16 and 28 under 35 USC § 103 as being obvious over the Yan reference in view of Grawrock (U.S. Patent Pub. No. 2004/0117625), and claim 30 under 35 USC § 103 as being obvious over the Yan reference in view of the Pinkas reference. Applicants respectfully traverse the Section 103 rejections insofar as they may be applied to the claims as amended.

To remind the Examiner, the present application addresses the situation where two computing entities are to interact and a first one of the entities is required to proffer a showing to the second entity such that the second entity can decide whether to trust the first entity. As part of the proffering, the first entity, which typically includes an executable, includes a code ID associated therewith. As is set forth in the specification of the present application at about paragraphs [0025]-[0028], the code ID 16 for a particular first entity 10 is derived or calculated from a digest of [the executable of] the first entity 10 and security information relating thereto such as an ID 18 (which is referred to in the claims as the security ID), and is typically a hash of the code ID 16 and the ID 18 in a manner akin to that which is employed in a digital signature.

The security information in the ID 18 specifies security-related aspects of the operation of the first entity 10, which as shown in Fig. 2 may be set forth as a number of name-value security attribute parameters. In particular, if the first entity 10 wishes to modify its security environment such as for example by reading in a file, opening a debugging port, and the like, the first entity 10 is itself responsible for doing so. However, if a developer developing the first entity 10 wishes to have a particular behavior parameterized, and the parameter has security

implications (e.g., open a different file based on program input, or debug based on program input) then the parameter can be placed in the ID 18 and the executable of the first entity 10 can be written to refer only to the ID 18 for the parameter. Thus, although the parameter could potentially be modified within the ID 18 by a nefarious entity, the modified ID 18 will cause the hash of the calculated code ID 16 to change, where such change can be interpreted by an interested party such as the second entity 12 as an indication that the first entity 10 should not be trusted.

Accordingly, independent claim 31 as amended recites the use of such a code ID to allow a second entity to trust a first entity. In particular, in claim 31, an attestation message is transmitted from a first computer entity to a second computer entity, where the attestation message includes a code ID associated with the first computer entity that is calculated by using a security ID associated with the first computer entity. The security ID is ensured to have not been tampered with by verifying the validity of the transmitted code ID, and a trust message is then transmitted from the second computer entity to the first computer entity upon successful verification. Notably, claim 31 as amended recites that the security ID (i.e., the ID 18) includes security information relating to the first computer entity, where the security information is expressed as a number of name-value security attribute parameters, and that the first computer entity is an executable and refers to the parameters in the security information in the security ID to determine whether particular security behavior is allowed. Also, claim 31 as amended recites that the code identifier (code ID) is representative of the first computer entity and is calculated as a one-way hash of a combination of the executable of the first computer entity and the security ID so that modification of the security information in the security ID causes the calculated code ID to change and the second computer entity can interpret the change as an indication that the first computer entity should not be trusted.

Independent claim 30 also recites the code ID of claim 31, albeit in the context of a method of establishing trust between a first computer entity and a server, where a first computer entity seeks a granting of trust from a server by sending an inquiry in the form of a can-attest message to the server. The can-attest message states that the first computer entity can send an

attestation message but that the first computer entity would like to know from the server whether such an attestation message is required, and if so any requirements that such server has with regard to such attestation message. In response, the server sends an attestation-wanted message to the first computer entity, where the attestation-wanted message states that the server does in fact require an attestation message from the first computer entity and that the attestation message as sent by the first computer entity must adhere to certain requirements as defined in such attestation-wanted message. Notably, one of the certain requirements of claim 30 as amended is that the attestation message is to include the aforementioned code ID associated with the first computer entity.

As the Examiner notes, the Yan reference discloses at about paragraph [0060] that when an application [first entity] wants to attest its validity to a remote server [second entity], the application sends integrity metrics including C_A, which is a hash of the executable image of the application. Applicants respectfully submit, however, that the Yan reference does not disclose or suggest that C_A is a one-way hash of such executable image and a security ID, as is now recited in claims 30 and 31, or that such a security ID should or could include security information relating to the application, where the security information is expressed as a number of name-value security attribute parameters that the Yan application refers to in order to determine whether particular security behavior is allowed, as is also now required by claims 30 and 31. Likewise, the Yan reference does not at all appreciate that by calculating such a code ID, modification of the security information in the security ID causes the calculated code ID to change and the Yan remote server can interpret the change as an indication that the Yan application should not be trusted, as is further required by claims 30 and 31.

As the Examiner also notes, the Yan reference also discloses the use of messages 302-308 for the purpose of establishing a trust relationship. In particular, such messages represent initial attestations to establish trust in a general sense, and further attestations to establish trust 'for a special purpose' (Yan at [0064]). Applicants respectfully note however, that none of the Yan messages 302-308 are preliminary messages that establish *prior to the sending of an attestation* whether attestations are even necessary, particularly in the manner recited in claim

30. Specifically, none of the Yan messages is disclosed or even suggested as being an inquiry to a server in the form of a can-attest message that states that a first computer entity can send an attestation message, but that the first computer entity would like to know from the server whether such an attestation message is required, and if so any requirements that such server has with regard to such attestation message, or as being a response from the server in the form of an attestation-wanted message stating that the server does in fact require an attestation message from the first computer entity and that the attestation message as sent by the first computer entity must adhere to certain requirements as defined in such attestation-wanted message, all as is required by claim 30. Instead, the Yan system presumes that the attestations of 302-304 or 306-308 are required, and therefore does not allow for any such can-attest or attestation-wanted messages *prior to* such Yan attestations.

The Examiner cites to the Pinkas reference as disclosing the use of an initial attestation method. However, in the Pinkas system, a first party requests an attestation from a second party and in response the second party sends the attestation. Applicants respectfully point out that the Pinkas system does not require or even suggest the use of any prior can-attest message *from such a second party to such a first party* that states that the second party can send such an attestation message but that the first computer entity would like to know from the server whether such an attestation message is required, and if so any requirements that such server has with regard to such attestation message, or that the first party *in response to such a can-attest message* sends an attestation-wanted message, particularly as is required by claim 30. Instead, the Pinkas second party sends an attestation at the behest of the Pinkas first party, without the option for the Pinkas second party to inquire as to whether an attestation is needed.

Applicants respectfully note that the Qui reference is cited primarily as disclosing a period of time for which a secret is valid, and that the Grawrock reference is cited primarily as disclosing a sealing function. That said, Applicants respectfully submit that the Qui and Grawrock references are otherwise inapposite to the claims of the present application.

Thus, Applicants respectfully submit that the Yan, Pinkas, Qui and Grawrock references cannot be combined to make obvious the subject matter variously recited in independent claims

30 and 31. Accordingly, Applicants must conclude that such references cannot be applied to make obvious such claims 30 and 31 as amended or any claims depending therefrom, including claims 2-4, 7-12, 14, 18-21, 23, 25-27, 29, 32, 33, and 36-38. Moreover, inasmuch as claims 30 and 31 have been shown to be non-obvious, then so too must all claims depending therefrom including claims 16 and 28 be non-obvious at least by their dependencies. As a result, Applicants respectfully request reconsideration and withdrawal of the Section 103 rejections.

CONCLUSION

In view of the foregoing Amendment and Remarks, Applicants respectfully submit that the present application including claims 2-4, 7-12, 14, 16, 18-21, 23, 25-33, and 36-38 is in condition for allowance and such action is respectfully requested.

Respectfully Submitted,

Date: April 5, 2010

/Joseph F. Oriti/
Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439